Fábrica de Noobs

Desmistificando: aviso de "misantropia"

Natanael Antonioli

Junho de 2026

1. SUMÁRIO

2. Com o que estamos lidando? 3

3. Como o ataque foi realizado? 4

4. Como sabemos que *Misantropo* está falando a verdade? 10

5. O ataque foi feito para divulgar um álbum? 13

6. O que "misantropia" significa? 16

7. Há algum perigo real? 20

8. Conclusões 22

2. COM O QUE ESTAMOS LIDANDO?

Nas primeiras horas do dia 20 de julho de 2026, brasileiros relataram mensagens enigmáticas em seus celulares transmitidas como avisos da Defesa Civil que continham a palavra "misantropia", ou variações dela.

As mensagens **foram reportadas a partir de 1:20 da manhã do dia 20 de julho de 2026**, e chegaram na forma de alerta de emergência, de mensagem de texto e de mensagem no *WhatsApp* para pessoas em múltiplos estados do Brasil. Como o *Google* se vale de alertas da Defesa Civil, a mensagem também apareceu em serviços com o *Google Maps*.

Figura 1: mensagens recebidas.

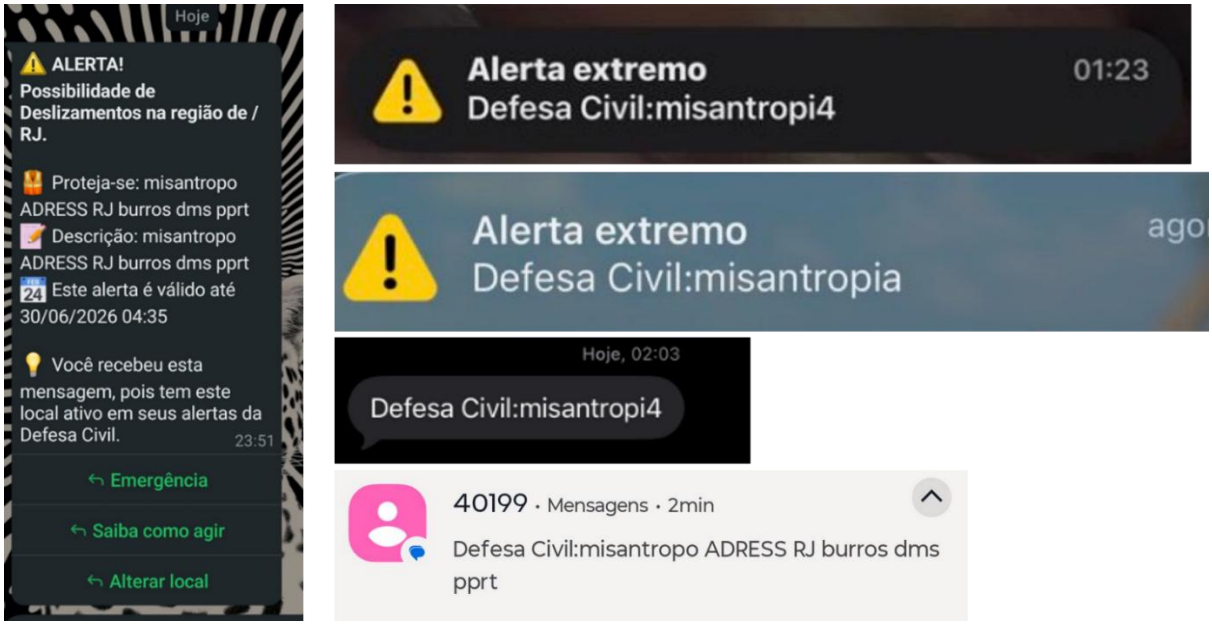
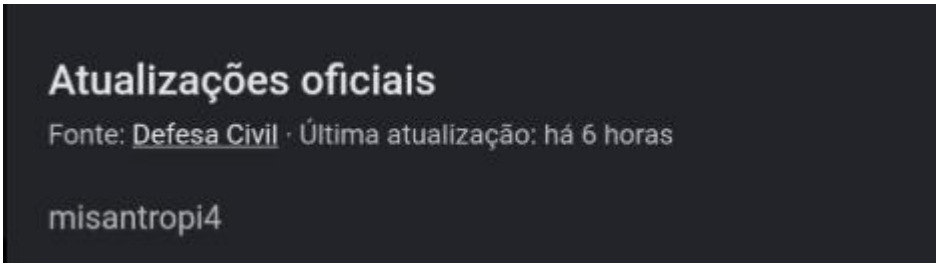


Figura 2: alerta no *Google Maps*.



3. COMO O ATAQUE FOI REALIZADO?

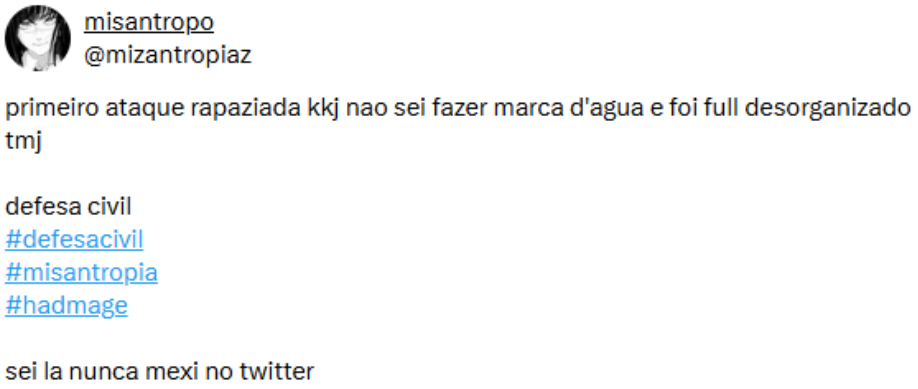
Todo tipo de ataque cibernético **ocorre quando há uma vulnerabilidade presente**, que pode se apresentar em diversas naturezas. Há diversas vulnerabilidades – cuja exploração é simples ou complexa – que, se existentes, possibilitariam o ataque. Porém, nesse caso, **possuímos informações adicionais que nos permitem detalhar sua execução**.

Tais alertas são emitidos através da *Interface de Divulgação de Alertas Públicos* (IDAP, https://educacao.cemaden.gov.br/midiateca/interface-de-divulgacao-de-alertas-publicos-idap/), uma plataforma governamental que possibilita enviar alertas relacionados, normalmente, às emergências climáticas.

Os alertas por *SMS* ou *WhatsApp* **são enviados como mensagens comuns**, utilizando a rede móvel ou a internet. Porém, a principal função do sistema é usar a tecnologia *Cell Broadcast*, que **envia um sinal para antenas de uma dada região** que, então, **irão enviar sinais para os celulares que estiverem na área**. Essa função, projetada para alertas de emergência, funciona **mesmo sem conexão com a internet ou com a rede móvel de forma estável**, uma vez que **basta o envio de um único sinal aos celulares**.

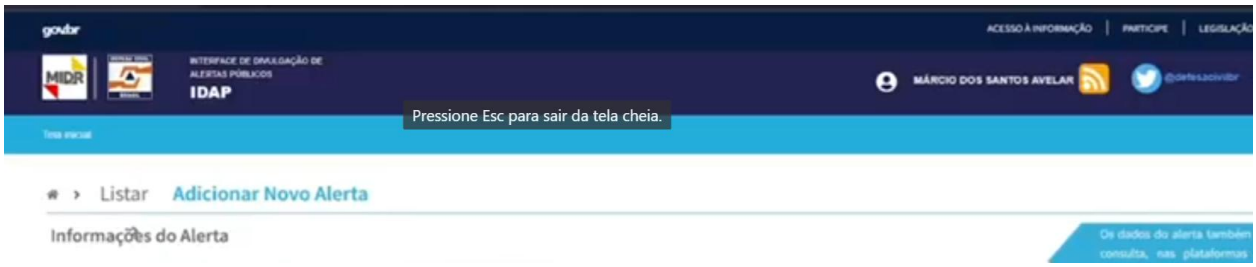
Porém, o alerta precisa ser disparado através de uma interface. De acordo com um usuário que assumiu a autoria (https://archive.is/8HRi8), o ataque **partiu dessa interface**. e, conforme verificaremos, ele **a sustentou com provas suficientes**

Figura 3: postagem acompanhada de um vídeo.



O vídeo (reenviado em https://x.com/who1sroot/status/2068231132441710893) mostra que o autor **acessou o sistema do IDAP usando credenciais privadas** e **seguiu o fluxo para criar um novo alerta**.

Figura 4: acesso ao sistema do IDAP.



Então, ele **escreveu a mensagem desejada** – no vídeo, vemos *misantropi4* e marcou o envio para a região desejada. O sistema permite selecionar por municípios em um estado, bairros em um município ou mapa, o que, efetivamente, **torna a abrangência de um ataque do tipo arbitrariamente grande**. Ele permitiu que o alerta fosse enviado também por outros meios, como *WhatsApp* e SMS.

Figura 5: marcação de abrangência.

Em seguida, o sistema **demandou que a senha do usuário fosse inserida novamente**, e a captura nos revela que **essa senha tinha apenas 6 caracteres** e **não envolvia nenhuma outra etapa de autenticação**.

Figura 6: envio da mensagem.

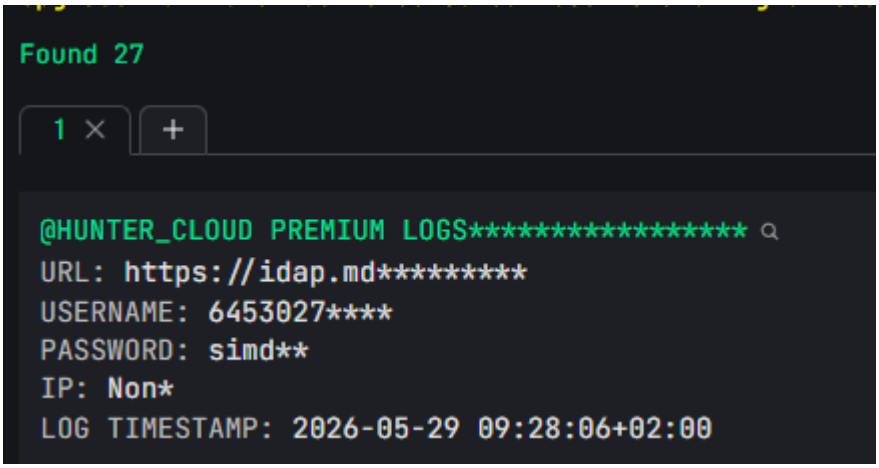
Assim, o ataque **foi realizado por meio da obtenção de credenciais de login** na plataforma do IDAP, algo constatado através da filmagem produzida. Mas, resta saber: como essas credenciais foram obtidas por um atacante?

Ataques cujo alvo seja planejado geralmente envolvem uma etapa de obtenção dessas credenciais através de engenharia social, o que requer que uma vítima seja convencida a compartilhar dados com um atacante. Uma tática comum envolve se passar por um funcionário da organização – como das áreas de suporte – e demandar dados de login de outros colaboradores que não conhecem protocolos de segurança.

Ao mesmo tempo, ataques contra pessoas ou instituições frequentemente em vazamentos de dados mais amplos, que não são usados para nenhum fim específico, mas **publicados ou vendidos na internet**. Sites como o *OSINTLeak* **registram esses vazamentos**, e parte do trabalho de segurança da informação envolve monitorá-los.

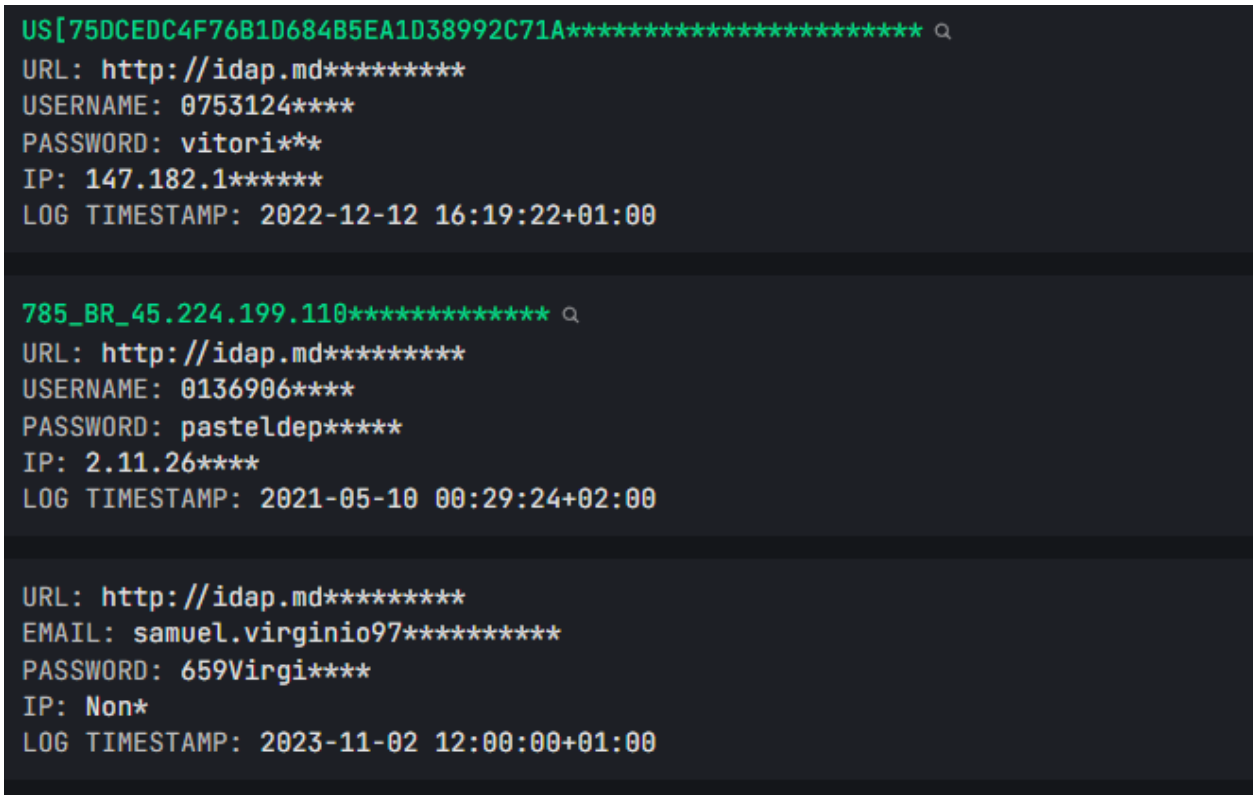
Aqui, o autor parece **ter obtido as credenciais de forma oportuna**, não de um ataque planejado. O *OSINTLeak* (https://app.osintleak.com/dashboard/search?redirect_uri=https://osintleak.com) **revela 27 credenciais vazadas, sendo uma de 29 de maio de 2026 e com senha de 6 dígitos**.

Figura 7: provável credencial utilizada.



Além disso, outras credenciais mostram que não há uma política de senhas seguras, já que **encontramos senhas com nomes próprios ou com substantivos comuns**, todas muito pouco complexas.

Figura 8: outras senhas vazadas.

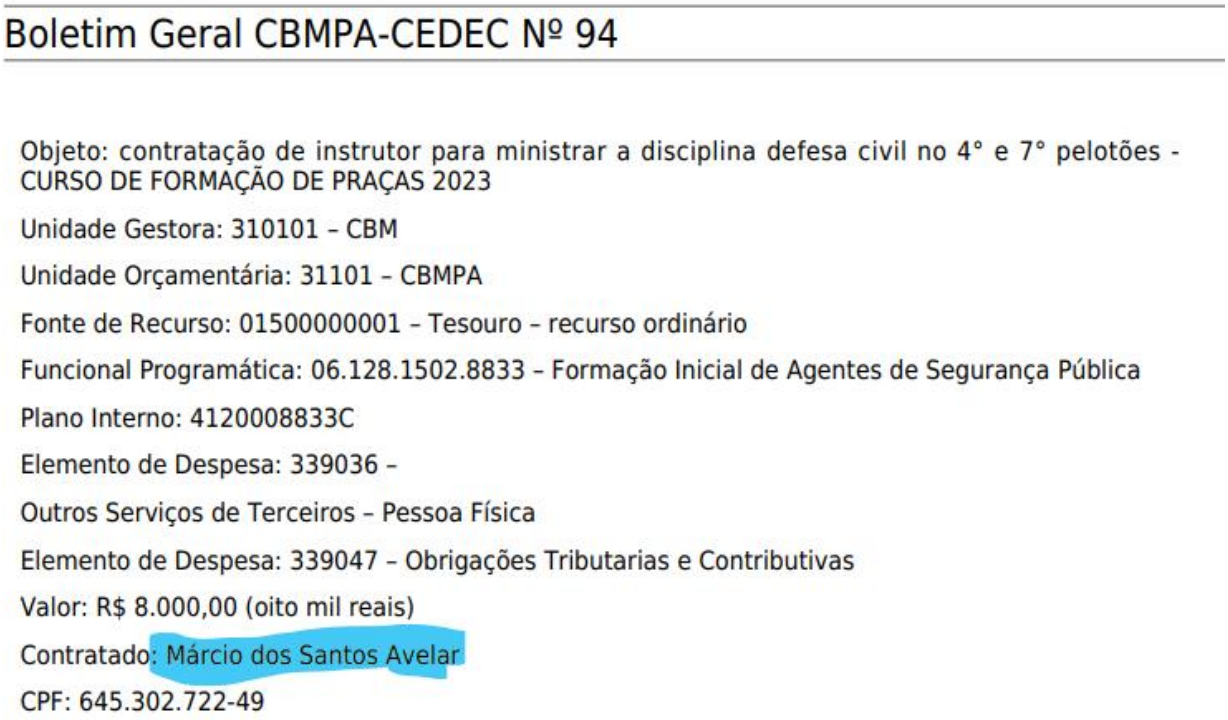


No vídeo, **vemos o usuário de Márcio dos Santos Avelar**. Ele **não é o autor do ataque**, mas sim um colaborador que possuía credenciais de acesso e as teve vazadas na internet.

Figura 9: usuário utilizado.

Documentos públicos de 2023 (https://siga.bombeiros.pa.gov.br/boletim.php?id=1868) trazem o nome de Márcio **associado ao Corpo de Bombeiros no Estado do Pará**, indicando que ele **ministrou uma disciplina de defesa civil**. Encontramos uma pessoa de mesmo nome que se graduou em Geografia em 2011 (https://www.escavador.com/sobre/1983585/marcio-dos-santos-avelar) pela *Universidade Federal do Pará*, sendo este provavelmente o proprietário das credenciais.

Figura 10: nome de Márcio em documento oficial público.



Boletim Geral CBMPA-CEDEC Nº 94

Objeto: contratação de instrutor para ministrar a disciplina defesa civil no 4° e 7° pelotões - CURSO DE FORMAÇÃO DE PRAÇAS 2023

Unidade Gestora: 310101 – CBM

Unidade Orçamentária: 31101 – CBMPA

Fonte de Recurso: 01500000001 – Tesouro – recurso ordinário

Funcional Programática: 06.128.1502.8833 – Formação Inicial de Agentes de Segurança Pública

Plano Interno: 4120008833C

Elemento de Despesa: 339036 –

Outros Serviços de Terceiros – Pessoa Física

Elemento de Despesa: 339047 – Obrigações Tributarias e Contributivas

Valor: R$ 8.000,00 (oito mil reais)

Contratado: Márcio dos Santos Avelar

CPF: 645.302.722-49

4. COMO SABEMOS QUE *MISANTROPO* ESTÁ FALANDO A VERDADE?

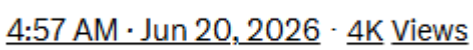
A informação dada anteriormente parte da premissa que um usuário no *X* (https://x.com/mizantropiaz/) de nome *Misantropo* foi o autor do ataque, e usa como sustentação **um vídeo produzido pelo próprio usuário mostrando as etapas realizadas**.

A razão pela qual a postagem dele foi considerada como prova suficiente **reside, justamente, no conteúdo da filmagem**, na qual verificamos o site sendo preenchido e os alertas sendo enviados através de sua interface. Sabemos que a imagem é do site oficial do IDAP porque ele condiz com os mostrados em materiais anteriores do governo (como em https://youtu.be/jG2Y-txJoXU?si=s3ytiHM5ke4P8z6m&t=2488).

Figura 11: site do IDAP visto em 2022, com a mesma interface.

É possível forjar um vídeo do tipo, mas há razões para supor que isso não ocorreu. Em primeiro lugar, a primeira postagem ainda existente do usuário sobre isso já mostrava o mesmo site (https://x.com/mizantropiaz/status/2068204965001068619), e **foi feita às 02:31 da manhã**, ao passo que a captura arquivada mostra o horário de 04:57 da manhã no fuso UTC, o que **se traduz para 01:57 da manhã no horário de Brasília**.

Figura 12: horário da postagem.



Forjar este vídeo iria requerer que **a interface do IDAP fosse clonada como um site local**, o que é relativamente simples de ser feito quando se possui acesso a todas as páginas. No entanto, o site do IDAP é restrito, o que significa que o autor do vídeo **ou teve acesso ao site do IDAP, ou o forjou através de semelhança visual**.

Se o autor teve acesso ao site do IDAP, então ele, efetivamente, **acessou a interface que permite envio de mensagens** – e o vídeo ser forjado seria equivalente a dizer que duas pessoas diferentes acessaram a parte restrita do site do IDAP, mas uma fez o ataque real, e outra apenas copiou o site para o computador e fez um ataque simulado.

Se o autor não teve acesso ao site do IDAP, então ele foi **capaz de copiar uma instrutura que permaneceu funcional durante a filmagem em apenas 40 minutos**, algo que parece improvável mesmo com o auxílio de ferramentas modernas. Ao passo que o fluxo mais rápido para essa proeza seria enviar capturas para uma inteligência artificial generativa e solicitar um clone, **demoraria certo tempo até obter um site funcional**.

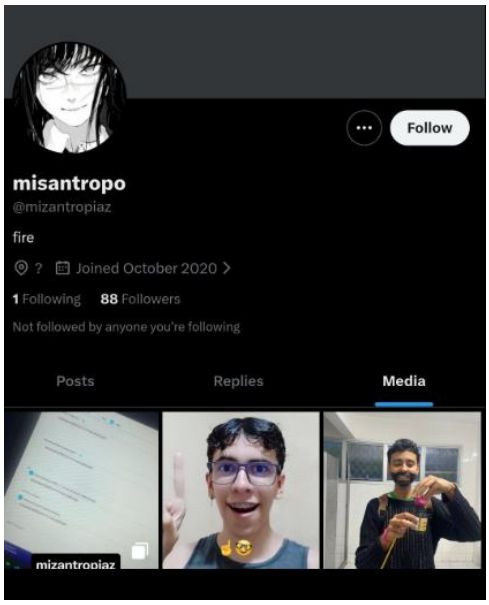
Na internet, muitos acusaram o autor de ser um *larper*, uma gíria que indica pessoa que se passa por conhecedora ou capaz mesmo não sendo. De fato, o autor desse ataque **não é um especialista em segurança** e **não usou nenhuma técnica avançada**, o que significa que, se ele se apresentar como tal, **é efetivamente um *larper***.

Porém, ele de fato **comprovou ter realizado esse feito**. Ao fazer isso, ele também, além de **confessar em um perfil na internet**, vazou sua conta do *Spotify* e identificação do *CapCut*, o que significa que **identifica-lo é um processo fácil**.

Figura 13: identificação do *CapCut*.

Figura 14: página do *Spotify*.

Figura 15: perfil no *X*.



5. O ATAQUE FOI FEITO PARA DIVULGAR UM ÁLBUM?

Paralelamente, outras pessoas se apropriaram do ataque para associar suas próprias produções pessoais. Por exemplo, um produtor musical alterou seu perfil no *Instagram* (https://x.com/Lucktvsx/status/2068194469518671886), inclusive publicando uma nota do governo federal feita com IA para indicar que o perfil seria removido.

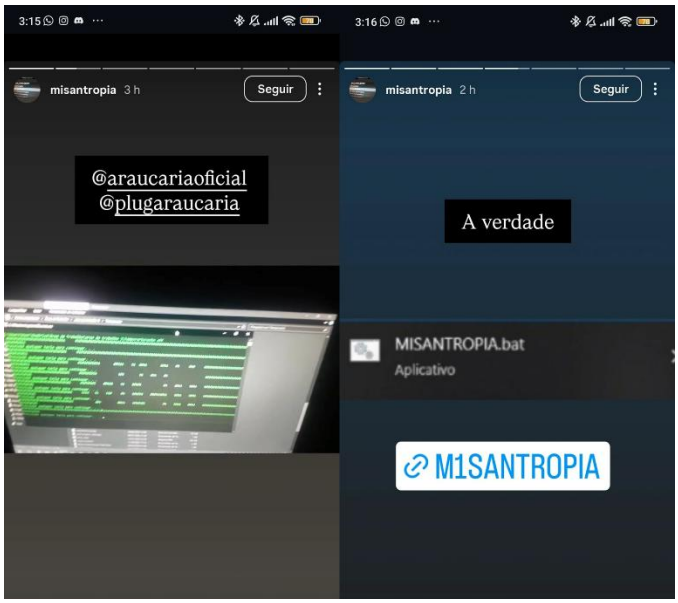
Figura 16: nota falsa.

misantropiaaa4
INSTAGRAM REMOVIDO
POR ORDEM DO GOVERNO FEDERAL
Este serviço foi removido do Brasil por descumprir a legislação brasileira e por se recusar a cumprir ordens judiciais.
A medida tem como objetivo proteger a população, combater crimes digitais e preservar a soberania e a segurança nacional.
A SEGURANÇA DO BRASIL EM PRIMEIRO LUGAR
A internet no Brasil deve ser um ambiente seguro, ético e responsável para todos.
Fundamentação legal:
Lei nº 12.965/2014 – Marco Civil da Internet
e demais legislações vigentes.
GOVERNO FEDERAL DO BRASIL
Unidos por um Brasil mais seguro.
Saiba mais em: www.gov.br
misantropiaaa4 Os posts serão mantidos mas o responsável pelo ataque cibernético ja foi vetado.
31 minutos atrás

Figura 17: brasão na nota falsa e brasão real.

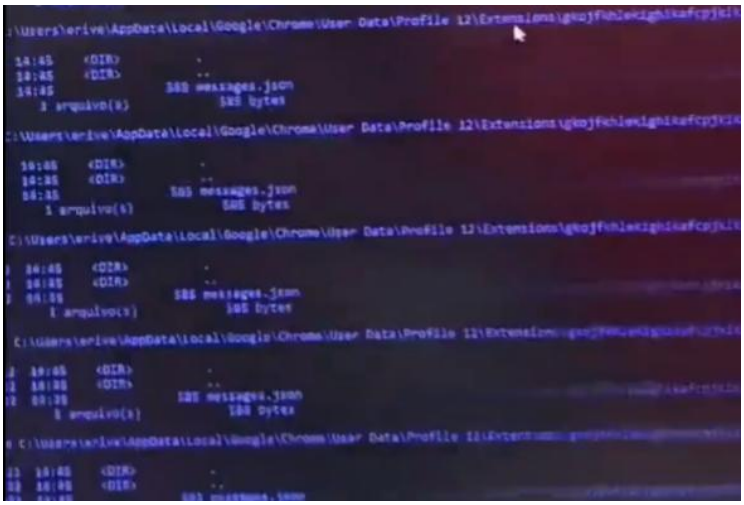
Tudo que o perfil postou para comprovar o feito foi um arquivo *.bat* e um terminal do *Windows* que mostrava seu nome artístico – esses sim **fáceis de serem produzidos rapidamente**.

Figura 18: publicações do perfil.



Outra pessoa postou (https://x.com/lilkavic888/status/2068240429686944190) um vídeo no qual o terminal do *Windows* muda rapidamente de texto. Porém, basta congelar a imagem para verificar que o autor apenas **criou um laço de repetição que mostra seus arquivos**.

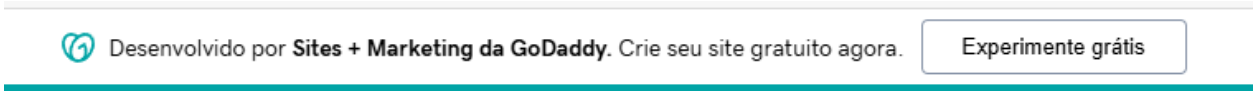
Figura 19: cena do vídeo.



Outro optou por registrar um site na internet com esse nome (https://misantropi4.com) mas, até o momento, **o site permanece em branco e é provavelmente uma tentativa de capitalizar com esse ataque**.

Figura 20: site em questão.

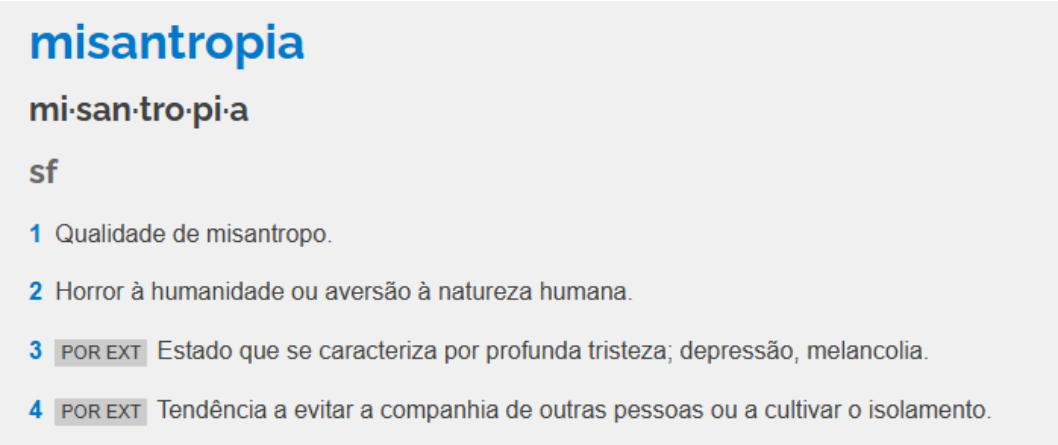
Figura 21: marca d'água da *GoDaddy*, um serviço de hospedagem.



6. O QUE "MISANTROPIA" SIGNIFICA?

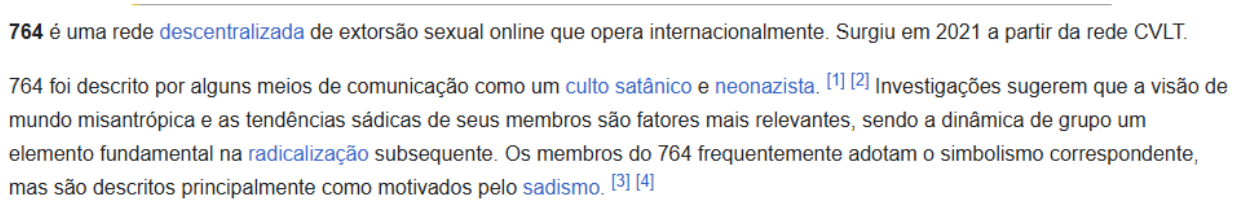
No dicionário (https://michaelis.uol.com.br/busca?id=RQvZd), o termo "misantropia" é definido como **aversão à humanidade, bem como a tristeza, depressão ou melancolia decorrente dela**.

Figura 22: definição do dicionário.


misantropia
mi·san·tro·pi·a
sf
1 Qualidade de misantropo.
2 Horror à humanidade ou aversão à natureza humana.
3 POR EXT Estado que se caracteriza por profunda tristeza; depressão, melancolia.
4 POR EXT Tendência a evitar a companhia de outras pessoas ou a cultivar o isolamento.

Alguns usuários extrapolaram para uma mensagem alienígena ou uma revolta de sistemas de inteligência artificial, já que ambos são entidades fora do contexto de humanidade. Outros, ainda, associaram ao grupo criminoso *764*, associado com extorsão sexual, zoofilia, tortura psicológica e extorsão, uma vez que o termo aparece na sua página da *Wikipedia*.

Figura 23: página sobre o grupo.


764 é uma rede descentralizada de extorsão sexual online que opera internacionalmente. Surgiu em 2021 a partir da rede CVLT.

764 foi descrito por alguns meios de comunicação como um culto satânico e neonazista. [1] [2] Investigações sugerem que a visão de mundo misantrópica e as tendências sádicas de seus membros são fatores mais relevantes, sendo a dinâmica de grupo um elemento fundamental na radicalização subsequente. Os membros do 764 frequentemente adotam o simbolismo correspondente, mas são descritos principalmente como motivados pelo sadismo. [3] [4]

Porém, até agora, o autor **não parece ter associações do tipo e sequer parece advogar por seus ideais**. A realidade parece muito mais mundana: a palavra "misantropia" e suas variações, como "misantropo" e "misantropi4" **são apelidos que ele escolheu para sua identidade *hacker* na internet**, uma prática extremamente comum entre iniciantes deste mundo.

Alguns () **mencionam que o termo é pouco comum**, mas uma pesquisa revela que ele surge em múltiplas discussões populares em português (https://www.reddit.com/r/opiniaoimpopular/comments/1h13whl/misantropia_deve_ser_normalizado/, https://cantodosclassicos.com/filmes-com-temas-niilistas-misantropos-e-cinicos/, https://fernandonogueiracosta.wordpress.com/2016/02/08/preciso-aprender-a-ser-so/, https://www.reddit.com/r/Filosofia/comments/y62yzc/como_voc%C3%AAs_enxergam_a_misantropiamisantropos/), que **é comum em certos ramos de filosofia popular e autoajuda**.

Figura 24: postagem de usuário.

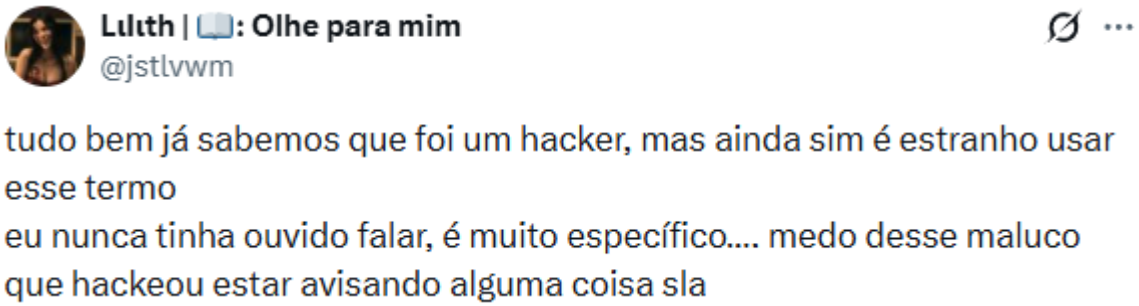

Lılıth | 📖: Olhe para mim
@jstlvwm
tudo bem já sabemos que foi um hacker, mas ainda sim é estranho usar esse termo
eu nunca tinha ouvido falar, é muito específico.... medo desse maluco que hackeou estar avisando alguma coisa sla

Figura 25: menção do termo.

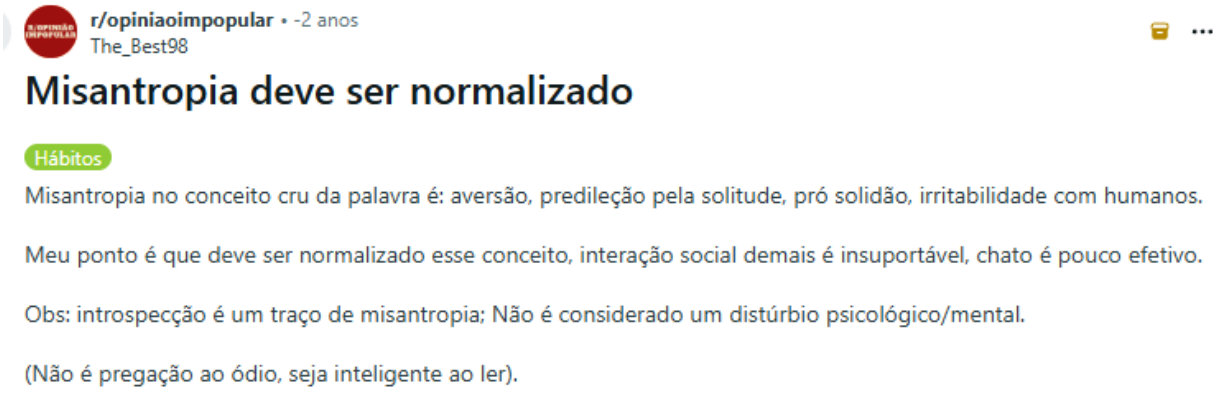
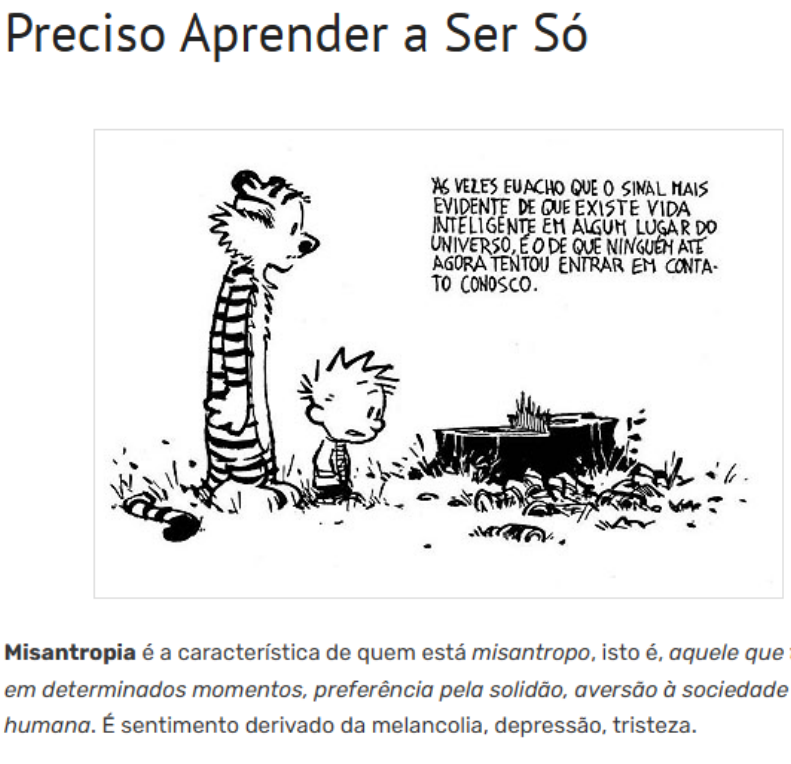

r/opiniaoimpopular • -2 anos
The_Best98
Misantropia deve ser normalizado
Hábitos
Misantropia no conceito cru da palavra é: aversão, predileção pela solitude, pró solidão, irritabilidade com humanos.
Meu ponto é que deve ser normalizado esse conceito, interação social demais é insuportável, chato é pouco efetivo.
Obs: introspecção é um traço de misantropia; Não é considerado um distúrbio psicológico/mental.
(Não é pregação ao ódio, seja inteligente ao ler).

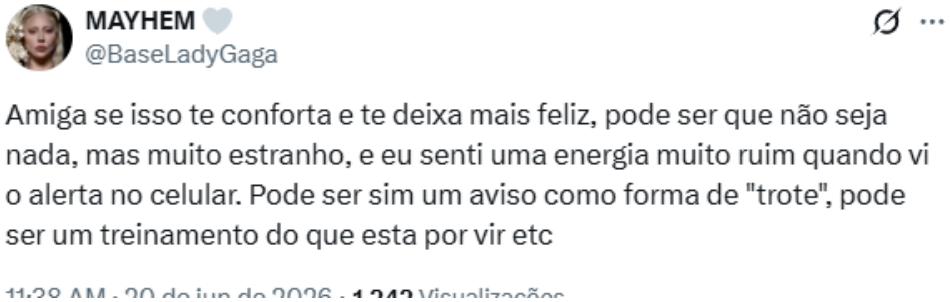
Figura 26: menção do termo.

Figura 27: menção ao termo.


Preciso Aprender a Ser Só
AS VEZES EUACHO QUE O SINAL MAIS EVIDENTE DE QUE EXISTE VIDA INTELIGENTE EM ALGUM LUGAR DO UNIVERSO, É O DE QUE NINGUÉM ATÉ AGORA TENTOU ENTRAR EM CONTATO CONOSCO.
Misantropia é a característica de quem está *misantropo*, isto é, *aquele que tem, em determinados momentos, preferência pela solidão, aversão à sociedade humana*. É sentimento derivado da melancolia, depressão, tristeza.

Outros (https://x.com/BaseLadyGaga/status/2068342673769951698) citam que sentiram uma sensação ruim ao ver a mensagem – mas isso **é esperado quando mensagens do tipo existem para alertar de perigos reais**, como incêndios, deslizamentos e enchentes.

Figura 28: postagem de um usuário.

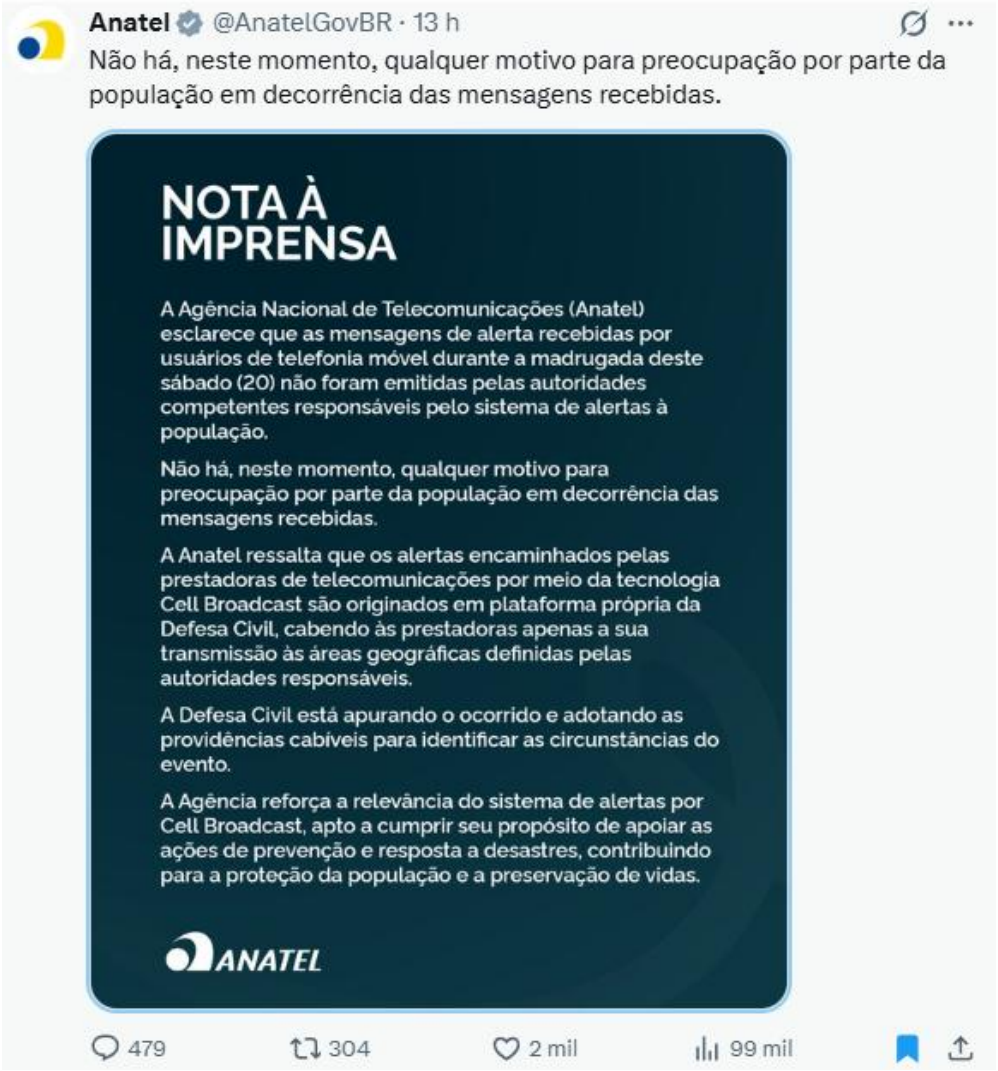

MAYHEM
@BaseLadyGaga
Amiga se isso te conforta e te deixa mais feliz, pode ser que não seja nada, mas muito estranho, e eu senti uma energia muito ruim quando vi o alerta no celular. Pode ser sim um aviso como forma de "trote", pode ser um treinamento do que esta por vir etc

7. HÁ ALGUM PERIGO REAL?

Não havia nenhum tipo de emergência real na madrugada do dia 20, o que significa que, em termos do que o sistema foi produzido para avisar, **estamos seguros**. **Não existem falhas conhecidas no protocolo que permitam invasão do dispositivo**, o que significa que, nesse quesito, também não há preocupação.

Porém, a postura oficial do governo (https://x.com/AnatelGovBR/status/2068324928370200722) **minimiza riscos reais**, pois uma pessoa não autorizada **foi capaz de utilizar um sistema governamental restrito.**

Figura 29: postagem da Anatel.


Anatel @AnatelGovBR · 13 h
Não há, neste momento, qualquer motivo para preocupação por parte da população em decorrência das mensagens recebidas.
NOTA À IMPRENSA
A Agência Nacional de Telecomunicações (Anatel) esclarece que as mensagens de alerta recebidas por usuários de telefonia móvel durante a madrugada deste sábado (20) não foram emitidas pelas autoridades competentes responsáveis pelo sistema de alertas à população.
Não há, neste momento, qualquer motivo para preocupação por parte da população em decorrência das mensagens recebidas.
A Anatel ressalta que os alertas encaminhados pelas prestadoras de telecomunicações por meio da tecnologia Cell Broadcast são originados em plataforma própria da Defesa Civil, cabendo às prestadoras apenas a sua transmissão às áreas geográficas definidas pelas autoridades responsáveis.
A Defesa Civil está apurando o ocorrido e adotando as providências cabíveis para identificar as circunstâncias do evento.
A Agência reforça a relevância do sistema de alertas por Cell Broadcast, apto a cumprir seu propósito de apoiar as ações de prevenção e resposta a desastres, contribuindo para a proteção da população e a preservação de vidas.
ANATEL
479
304
2 mil
99 mil

Um atacante poderia, por exemplo, **ganhar acesso ao sistema para notificar uma ordem de evacuação perante uma ameaça real, causando pânico**. Esse tipo de ataque **também poderia servir de base para outros ataques**, por exemplo, se passando por uma organização oficial para transmitir *malware* ou *phishing*.

Além disso, ao passo que esse ataque não diga muito sobre outros sistemas que sequer se baseiam em *login* (como a urna eletrônica), esse ataque **levanta preocupações perante sistemas que usam a mesma tecnologia**, como bases de dados jurídicas, financeiras e de saúde, uma vez que **permite o vazamento de informações sensíveis**.

Por fim, esse ataque **seria facilmente evitado através de políticas básicas de segurança da informação**, como o monitoramento por credenciais vazadas, o uso de autenticação de dois fatores e políticas de senhas seguras.

8. CONCLUSÕES

Assim, podemos concluir que o ataque observado no dia 20 de junho **foi possibilitado pelo vazamento de uma credencial ativa**, pertencente a um funcionário que tinha acesso ao sistema de envio de notificações da Defesa Civil. Ainda que **não represente ameaças de desastres** (reais ou fantásticos), ela é mais uma instância que **reflete o descaso do poder público perante a segurança de sistemas críticos**.